Umfassende Cybersecurity-Lösungen und Services

SPIE ICS AG

SPIE ICS AG
Freiburgstrasse 251
CH-3018 Bern

T.: +41 58 301 11 11

www.spie.ch

November 2023

Einleitung

Cyberbedrohungen werden immer ausgefeilter werden und sind mittlerweile allgegenwärtig, deswegen benötigen Unternehmen benötigen einen umfassenden Ansatz für ihre Cybersicherheit. Ausserdem entwickeln sich die Cyberbedrohungen ständig weiter. Eine ganzheitliche Cybersicherheitsmethode beinhaltet, die Sicherheit aus allen Blickwinkeln zu betrachten und alle Aspekte der Geschäftstätigkeit eines Unternehmens zu berücksichtigen. Aus diesem Grund hat SPIE ICS in der Schweiz einen umfassenden Ansatz entwickelt, der die drei Hauptaspekte der Cybersicherheitsresilienz berücksichtigt − die Befähigung der Mitarbeitenden, die Implementierung von Prozessen und moderne Technologien.

SPIE ICS bietet ein robustes Portfolio an Cybersicherheitsdienstleistungen und -lösungen zum Schutz Ihrer IT-Infrastruktur, zur Sicherung sensibler Daten und zur Aufrechterhaltung der Integrität Ihres Betriebs. Dieses Whitepaper gibt Ihnen einen Einblick in unsere Cybersicherheitsangebote, Methoden und Partnerschaften, die Sie in die Lage versetzen, eine widerstandsfähige Cybersicherheitsstruktur aufzubauen.

Harmonisierung von Personen, Prozesse und Technologien: SPIEs Triade-Ansatz zur Cybersicherheit

SPIE ICS in der Schweiz ist bestrebt, erstklassige Cybersicherheitsdienstleistungen anzubieten, die auf die individuellen Bedürfnisse jedes Unternehmens zugeschnitten sind. Unsere Partnerschaften und Allianzen ermöglichen es uns, einen herstellerunabhängigen Ansatz zu verfolgen, so dass wir Produkte und Dienstleistungen stets an die spezifischen Bedürfnisse unserer Kundschaft anpassen können. Die folgenden Abschnitte vermitteln ein Verständnis unseres Ansatzes. Dann gehen wir auf die Bandbreite der Vorteile ein, die diese Methode für Organisationen bietet, und warum SPIE der richtige Partner für Ihr Unternehmen ist. Im Kapitel «Unser Lösungsradar» geben wir Ihnen Einblicke in unser Dienstleistungsportfolio, das von der Risikobewertung bis hin zu fortschrittlichen Sicherheitslösungen reicht und Ihre digitalen Vorhaben umfassend schützt.

PERSONEN PROZESSE TECHNOLOGIEN

SPIE bringt menschliches Fachwissen, rationalisierte Arbeitsabläufe und Spitzentechnologie in Einklang

Bei der Cybersicherheit geht es nicht nur um Technologie. Vielmehr ist sie ein umfassender Weg, der Personen, Prozesse und Technologien in Einklang bringt. Indem alle drei Aspekte mit gleichem Fokus und gleicher Strenge behandelt werden, gewährleistet SPIE eine Cybersicherheit, die belastbar, anpassungsfähig und

zukunftssicher ist. Für Unternehmen bedeutet dies ein beruhigendes Gefühl, Vertrauen in die Infrastruktur und eine Grundlage für nachhaltiges Wachstum.

Personen

Der Mensch ist die erste Verteidigungslinie: Egal, wie fortschrittlich eine Technologie ist, menschliches Versagen bleibt eine kritische Schwachstelle in jedem Unternehmen. Durch Schulungen und Sensibilisierung stellt SPIE sicher, dass alle Mitarbeitenden die Bedrohungen verstehen und in der Lage sind, als erste Verteidigungslinie des Unternehmens zu agieren.

Rollenbasierte Zugangskontrollen: Nicht alle benötigen Zugang zu allen Informationen. SPIE legt Wert auf das Prinzip der geringsten Privilegien. Das bedeutet, dass SPIE sicherstellt, dass jede Person nur den Zugriff erhält, die sie benötigt. Damit vermeiden wir potenzielle Datenlecks.

Kontinuierliche Schulung: Die Cybersicherheit entwickelt sich ständig weiter. Regelmässige Schulungen sorgen dafür, dass Ihre Mitarbeitenden immer auf dem neuesten Stand sind, was die aktuellen Bedrohungen und bewährten Verfahren angeht.

Prozesse

Die Bedrohungen sind heutzutage vielfältig. Deshalb sind statische Sicherheitsprozesse eine Belastung. Aus diesem Grund entwickelt SPIE die anpassungsfähigen Sicherheitsprotokolle als Reaktion auf die neuesten Bedrohungsdaten stets weiter.

Plan zur Reaktion auf Vorfälle: Ein klar definierter Prozess, um Sicherheitsvorfälle zu erkennen, darauf zu reagieren und daraus zu lernen sorgt für eine rasche Eindämmung von Bedrohungen und eine Reduzierung der Ausfallzeiten.

Regelmässige Audits: Systematische Überprüfungen und Audits stellen sicher, dass die Sicherheitsmassnahmen wie vorgesehen funktionieren. Darüber hinaus zeigen sie verbesserungswürdige Bereiche auf.

Technologien

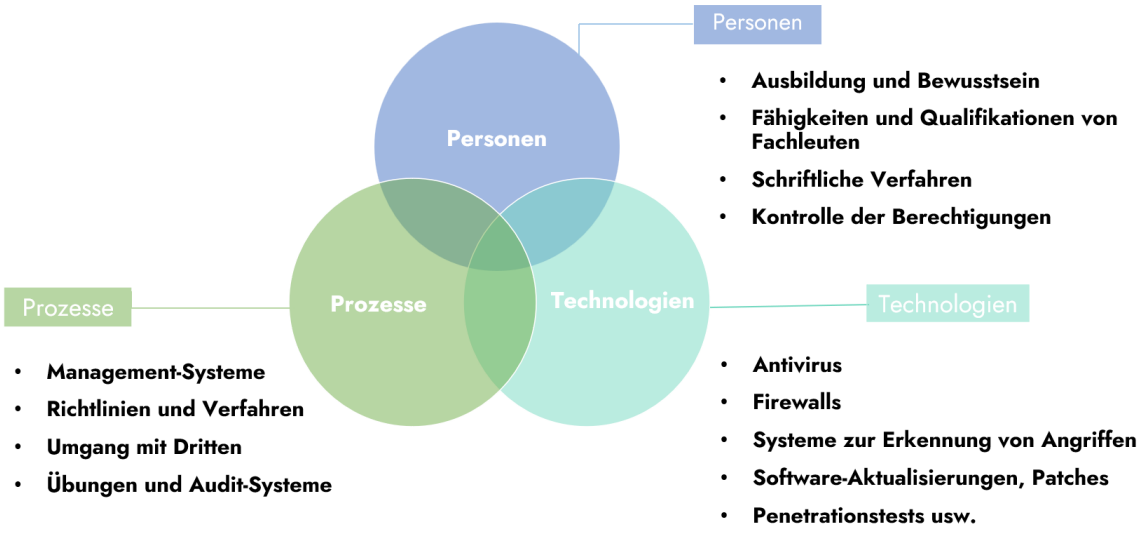
SPIE setzt moderne Technologie ein, um Anomalien und potenzielle Bedrohungen zu erkennen. Dies geschieht oft in Echtzeit, um schnelle Reaktionszeiten zu gewährleisten.

Sichere Infrastruktur: Von der Endpunktsicherheit bis zu sicheren Netzwerkarchitekturen investiert SPIE vorrangig in Technologien, die eine mehrschichtige Verteidigung gegen Cyberbedrohungen leisten.

Integration von KI und ML: Diese Technologien helfen bei der Vorhersage, Identifizierung und Abschwächung von Bedrohungen auf eine Weise, die zuvor unmöglich war. Durch

die Integration von künstlicher Intelligenz und maschinellem Lernen ist SPIE den Cyberangreifern immer einen Schritt voraus.

Die drei Hauptverteidiger



Im Wesentlichen schützt ein ganzheitlicher Ansatz für die Cybersicherheit durch die Integration von Personen, Prozessen und Technologien das Unternehmen nicht nur vor unmittelbaren Bedrohungen, sondern schafft auch die Voraussetzungen für einen nachhaltigen, langfristigen Erfolg. Demnach ist der Ansatz eine Investition in die Gegenwart und in die Zukunft.

Die Säulen einer sicheren digitalen Transformation: Ihre wichtigsten Vorteile

Digitales Vertrauen (Digital Trust)

Digitales Vertrauen ist die Grundlage, auf der moderne Unternehmen gedeihen. Es ist mittlerweile unverzichtbar.

Die Kultivierung von digitalem Vertrauen führt zu einer gefestigten Markenreputation, die es Unternehmen ermöglicht, als verlässliche Partner in der digitalen Landschaft anerkannt zu werden. Eine vertrauenswürdige digitale Präsenz fördert eine tief verwurzelte Loyalität, die dazu führt, dass Kundinnen und Kunden nicht nur wiederkommen, sondern sich auch für die Marke einsetzen. Der Ruf, ein zuverlässiger digitaler Partner zu sein, kann ein Unternehmen von anderen abheben und ihm einen einzigartigen Wettbewerbsvorteil verschaffen.

Als Inhaber der ISO 27001-, 9001- und 14001-Zertifizierung ist SPIE ICS Ihr vertrauenswürdiger Partner, der Ihr Unternehmen unterstützt und ihm zu Erfolg verhilft.

Einhaltung von Vorschriften

In einer Welt der sich ständig weiterentwickelnden Vorschriften ist die Einhaltung derer nicht nur eine Anforderung, sondern ein strategischer Vorteil.

Die Einhaltung von Vorschriften gewährleistet einen unterbrechungsfreien Betrieb − frei von behördlichen Eingriffen oder unvorhergesehenen Unterbrechungen − und eliminiert das Risiko, dass finanzielle Strafen verhängt werden. Eine konforme Haltung stärkt zudem die Integrität einer Marke und die öffentliche Wahrnehmung und das Vertrauen der Stakeholder.

SPIE ICS unterstützt Sie auf Ihrem Weg zur Einhaltung der Vorschriften: mithilfe von ISMS-Beratern, verwalteten Sicherheitsdiensten und der Implementierung von Lösungen, die moderne Sicherheitstechnologien nutzen.

Verfügbarkeit von Kompetenzen

Das Fachwissen eines Teams ist die erste und wichtigste Verteidigungslinie einer Organisation.

Durch die Förderung eines gut ausgebildeten Teams können Unternehmen die Risiken, die sich aus unbeabsichtigten menschlichen Fehlern ergeben, drastisch reduzieren. Da Cyberbedrohungen immer vielfältiger werden, sorgt ein qualifiziertes Team ausserdem dafür, dass das Unternehmen flexibel bleibt und die Abwehrmassnahmen bei Bedarf aktualisiert.

SPIE ICS verfügt über zahlreiche hochqualifizierte und zertifizierte Ingenieurinnen und Ingenieure, die Ihre Organisation und Ihre Teams dabei unterstützen, das Wissen und die Fähigkeiten zur Cybersicherheit auszubauen.

Cyberresilienz

Angesichts der ständig wachsenden Cyberbedrohungen ist Resilienz die Rüstung, welche die Geschäftskontinuität schützt. Resiliente Systeme garantieren, dass Unternehmen auch dann betriebsbereit bleiben, wenn es von Cyberbedrohungen überschattet wird.

Resilienz bedeutet nicht nur, einen Sturm zu überstehen, sondern auch, sich schnell davon zu erholen und minimale Ausfallzeiten sicherzustellen. Eine widerstandsfähige Haltung verhindert Sicherheitsverletzungen, die zu direkten finanziellen Verlusten oder indirekten Verlusten aufgrund von Rufschädigung führen können. Ein widerstandsfähiges Unternehmen strahlt Vertrauen aus und gibt allen Beteiligten die Gewissheit, dass es in der Lage ist, Cyberangriffen zu widerstehen.

Unsere Mitarbeitenden, unsere Prozesse und unsere Technologien machen SPIE ICS zum Partner Ihrer Wahl, um die Widerstandsfähigkeit Ihres Unternehmens zu erhöhen. Dadurch helfen wir Ihnen, auch in schwierigen Zeiten erfolgreich zu sein.

Warum SPIE?

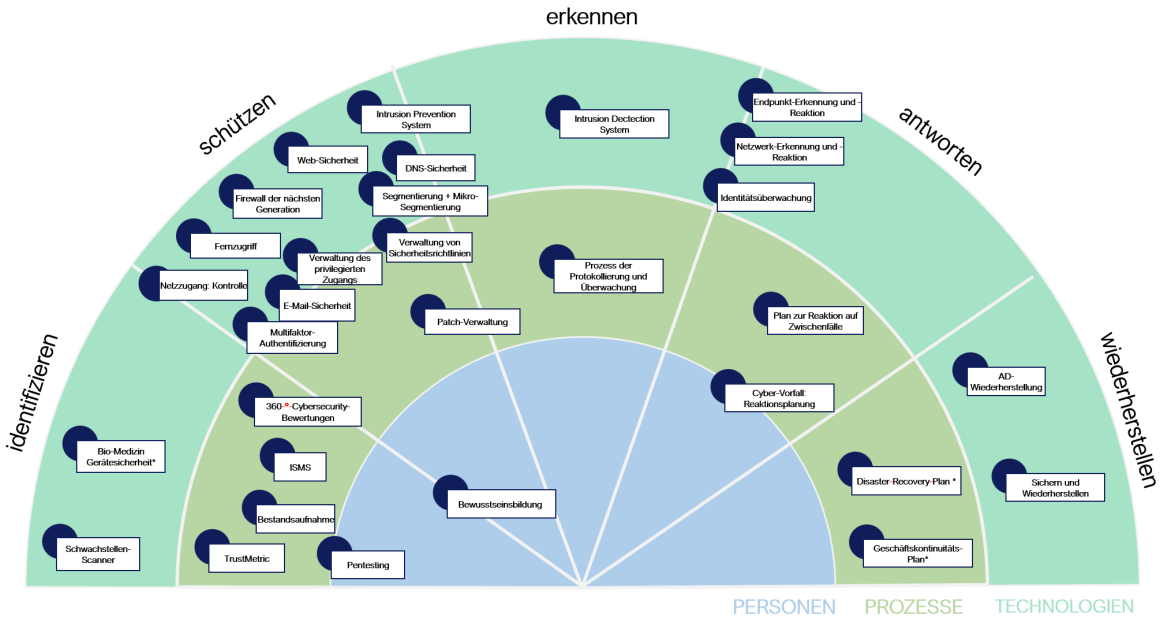
Wir sind uns der sich ständig weiterentwickelnden digitalen Landschaft bewusst, in der wir uns bewegen. Dementsprechend entwickeln wir uns ständig weiter. Wir stellen Ihnen vor, warum wir der optimale Partner für die Cybersicherheit Ihres Unternehmens sind. Diese Merkmale heben uns von Wettbewerbern auf dem Markt ab:

- **Hervorragender Service:** Wir sind stolz darauf, erstklassige Dienstleistungen anzubieten und sicherzustellen, dass jeder Auftrag höchsten Qualitätsstandards entspricht.
- **Erfahrene Ingenieurinnen und Ingenieure:** Unser Team ist nicht nur qualifiziert, sondern auch das Beste in der Cybersicherheit. Mit SPIE arbeiten Sie mit erfahrenen Expertinnen und Experten zusammen, die sich der Bereitstellung unvergleichlicher technischer Lösungen verschrieben haben.
- **Vielseitigkeit in verschiedenen Bereichen:** Unsere unterschiedlichen Dienstleistungen zeigen unsere Flexibilität und unsere Fähigkeit, auf unterschiedliche Bedürfnisse einzugehen. Dadurch bringen wir eine Fülle von branchenübergreifendem Wissen mit.
- **Finanziell solide:** Als Teil einer grossen, finanziell stabilen Gruppe gewährleisten wir Zuverlässigkeit und Langlebigkeit in allen unseren Partnerschaften. Sie können auf unsere dauerhafte Präsenz und unser Engagement vertrauen.
- **Unschlagbare Reaktionsfähigkeit:** Im Vergleich zu unseren grössten Konkurrenten zeichnen wir uns durch eine schnelle Reaktionszeit aus. Dank sechs Standorten in der ganzen Schweiz garantieren wir, dass wir in weniger als zwei Stunden bei Ihnen vor Ort sind.
- **Rund-um-die-Uhr-Support:** Unser Engagement für Sie ist unermüdlich. Mit 24/7-Support sind wir an jedem Tag der Woche für Sie da, wenn Sie uns brauchen.
- **Nischenkompetenz:** Zusätzlich zu unserem breiten Spektrum an Dienstleistungen verfügen wir über spezielles Fachwissen in bestimmten Bereichen. So stellen wir sicher, dass Sie in diesen Bereichen nur das Beste bekommen.
- **Massgeschneiderte Lösungen:** Bei SPIE gibt es keine Einheitslösung. Wir analysieren sorgfältig Ihre Umgebung und bieten Lösungen an, die Ihren spezifischen Anforderungen am besten entsprechen.
- **Herstellerneutral:** SPIE ICS bietet herstellerneutrale ICT-Lösungen. Wir passen Technologielösungen an Ihre spezifischen Bedürfnisse an. Unsere Dienstleistungen umfassen Planung, Implementierung sowie Wartung und Produktivität: Alles davon ist sicherheitsorientiert
- **Kundenerlebnis:** Wir kombinieren datengestützte Erkenntnisse, innovative Technologien und einfühlsame menschliche Interaktionen, um Ihre Erwartungen zu übertreffen. Letztlich fördern wir dadurch vertrauensvolle, langjährige Partnerschaften.


IMPLEMENTATION
Project Management
Installation, Configuration
Migration
Training/Handover
OPERATION
Managed Service
Incident Management
Proactive/reactive maintenance
OPTIMIZATION
Security policies
Technical resources
Sustainability
CUSTOMER EXPERIENCE
Cybersecurity Assessment
User Awareness
Security Strategy & Architecture
CONSULTING
Cybersecurity Assessment
User Awareness
Security Strategy & Architecture

Unser Lösungsradar

Unseren Lösungsradar haben wir entwickelt, damit Unternehmen ihre digitalen Werte und ihren Ruf durch unterschiedliche Strategien schützen können. Dieses Kapitel befasst sich mit dem Lösungsradar: den Komponenten einer umfassenden Cybersicherheitsstrategie. Dabei geht es zum einen um das Verständnis und die Bewertung potenzieller Bedrohungen durch die Cybersicherheit-Risikobewertung, zum anderen um die Verstärkung der Verteidigung mit modernen Lösungen wie Next Generation Firewalls. Wir erforschen die Bedeutung des Nutzerbewusstseins beim Aufbau von Cyberresilienz, die Wichtigkeit von sicheren Zugangskontrollen und die zentrale Rolle der Expertenaufsicht in Form von CISO as a Service. Jedes Thema, das hier behandelt wird, zeigt nicht nur eine einzelne Facette der Sicherheit, sondern ist ein integraler Bestandteil des übergreifenden Puzzles, das Sicherheit und Reaktionsfähigkeit in der Digitalität gewährleistet. Im Folgenden stellen wir Ihnen die Themen vor, mithilfe derer sie den Grundstein für eine sichere digitale Zukunft legen.



Bewertung des Cybersicherheitsrisikos: Umfassende Bewertung von Bedrohungen

Cyberbedrohungen zu verstehen und ihnen präventiv zu begegnen, ist nicht nur eine Notwendigkeit − es ist ein geschäftliches Muss. SPIE hat dies erkannt und bietet deshalb einen 360-°-Cybersecurity-Assessment-Service an.

Bei SPIE geht es nicht nur um die Identifizierung einzelner Schwachstellen, sondern um das Verständnis des Gesamtbildes. Wir bewerten sowohl interne als auch externe Bedrohungen und prüfen alle potenziellen Angriffspunkte. Im Rahmen einer umfassenden Risikobewertung bewerten wir zudem den Reifegrad Ihrer Cybersicherheit, identifizieren

Risiken und geben umsetzbare Empfehlungen. SPIE ICS in der Schweiz folgt dabei internationalen Standards wie ISO/IEC 27001, CIS Controls, NIST SP-800 und Swiss IKT.

Anhand des 360° Cybersecurity-Assessment-Services:

- erhalten Sie Einblicke in den Reifegrad Ihrer Governance und Ihrer Prozesse. Anhand von Interviews und Kurzüberprüfungen bestätigen wir, dass Ihre Cybersicherheit gemäss den besten Praktiken und Standards implementiert ist.
- überprüfen wir den Sicherheitsstatus Ihrer On-Premises- und Cloud-Infrastrukturtechnologie. Mithilfe von umfassenden Tests und Überprüfungen stellen wir sicher, dass die Kontrollen wirksam sind.
- bewerten wir das Bewusstsein Ihrer Mitarbeitenden und bieten Schulungen an.
- erfahren Sie den Cybersicherheitsrisikograd Ihres Unternehmens und erhalten eine Liste konkreter Massnahmen, um das Risiko effektiv und effizient zu mindern.

Aufgrund der Ergebnisse empfehlen wir unter Umständen zusätzliche Massnahmen in der Protokollierung und Überwachung von Prozessen, der Patch-Verwaltung oder der Bestandsverwaltung. Dies behandeln wir separat oder im Rahmen des Audits.

SPIE unterstützt Sie zudem bei der Erstellung eines Incident-Response-Plans, eines Disaster-Recovery-Plans und eines Business-Continuity-Plans: sowohl für die Prozesse als auch für die Tools.

Unser 360-°-Cybersecurity-Assessment-Service «Comprehensive Threat Evaluation» ist mehr als nur eine Bewertung − es ist ein strategisches Werkzeug, das Unternehmen in die Lage versetzt, die vielschichtigen Bedrohungen zu verstehen, vorherzusagen und ihnen effektiv zu begegnen. Mit SPIE als Partner schützen Sie nicht nur Ihre Gegenwart, sondern stärken auch Ihre Zukunft.

Pentesting: Evaluierung Ihrer Sicherheitslage

Ein effektiver Weg, die Bereitschaft einer Organisation zur Cyberverteidigung zu messen, sind Penetrationstests, die auch als Pentesting bezeichnet werden. Das Angebot von SPIE erlaubt es Unternehmen, ihre Sicherheitsmassnahmen in realen Szenarien objektiv zu bewerten.

Pentesting ist ein systematischer und kontrollierter Prozess zur Bewertung der Sicherheit eines Computersystems, eines Netzwerks oder einer Anwendung, indem Angriffe simuliert werden. Das Team von SPIE das aus ethischen Hackerinnen und Hackern sowie aus Cybersicherheitsexpertinnen und Cybersicherheitsexperten besteht, setzt hochentwickelte Techniken ein, um reale Cyberangriffe zu simulieren. So gewährleistet es eine umfassende Bewertung Ihrer Verteidigungsmechanismen. Über die oberflächlichen Schwachstellen hinaus dringt unser Team tief in Ihre Systeme ein. Es deckt versteckte Schwachstellen auf, die bei mehrschichtigen Angriffen ausgenutzt werden könnten. Unser Ziel ist es, potenzielle Eintrittspunkte zu finden, die böswillige Akteurinnen und Akteure nutzen könnten, um sich unbefugten Zugang zu verschaffen oder sensible Informationen zu kompromittieren. SPIE bietet dabei einen klaren Fahrplan für die Verbesserung Ihrer Sicherheitslage, um Ihnen zu erlauben, rasche und wirksame Massnahmen zu ergreifen. Durch eine Reihe kontrollierter Tests hilft Pentesting Ihrem Unternehmen dabei, Sicherheitslücken zu erkennen und zu beheben, seine allgemeine Cybersicherheitslage zu verbessern und sich gegen potenzielle Cyberbedrohungen zu schützen.

Zusammenfassend lässt sich sagen, dass der Pentesting-Service von SPIE Unternehmen eine wichtige Linse bietet, durch die sie ihre Cybersicherheitsmassnahmen betrachten und verbessern. Mit SPIE identifizieren Sie nicht nur Schwachstellen in Ihrem Unternehmen, sondern wandeln sie in Stärken um.

SPIE ICS bietet in der Schweiz Pentesting in verschiedenen Varianten an. Für weitere Informationen kontaktieren Sie bitte info.ch@spie.com

Security Awareness as a Service: Aufbau von Cyberresilienz

Technologische Schutzmassnahmen sind unbestreitbar wichtig. Oft wird jedoch das menschliche Verhalten übersehen, das ohne ein entsprechendes Bewusstsein ungewollt zu einem schwachen Glied in der Sicherheitskette werden kann. SPIE hat diese kritische Dimension erkannt und bietet das Programm Security Awareness as a Service an: eine umfassende Initiative, die darauf abzielt, eine auf Cybersicherheit ausgerichtete Unternehmenskultur zu pflegen.

Je nach Ihren Bedürfnissen bieten wir massgeschneiderte Inhalte in E-Trainings und Vor-Ort-Schulungen zu bestimmten Themen an. Dadurch schaffen wir die theoretische Grundlage für die gewünschte Widerstandsfähigkeit Ihres Unternehmens. Ergänzt wird unser Programm durch gezielte und aktuelle simulierte Phishing-Angriffe. Mithilfe unserer Begleitmassnahmen wird das Sicherheitsbewusstsein Ihrer Mitarbeitenden weiter

gestärkt. Diese Begleitmassnahmen erinnern Ihre Mitarbeitenden an die Sicherheitsrisiken, ohne dass dabei zusätzlicher Aufwand entsteht. Über das individuelle Lernen Ihrer Mitarbeitenden hinaus konzentriert sich das Programm von SPIE auf die Förderung eines kollektiven Cybersicherheitsbewusstseins, das die gesamte Unternehmenskultur in eine Kultur der Wachsamkeit und Widerstandsfähigkeit verwandelt.

Das SPIE-Angebot «Security Awareness as a Service» ist ein Schulungsprogramm und eine transformative Reise zugleich. Durch die Vermittlung eines tiefgreifenden Bewusstseins und Verständnisses für Cyberbedrohungen auf allen Unternehmensebenen stellt SPIE sicher, dass alle Personen im Unternehmen zu proaktiven Verteidigerinnen und Verteidigern werden, die kollektiv zu einer verbesserten Sicherheitslage beitragen. Gemeinsam schaffen wir die erste und wichtigste Verteidigungslinie gegen Cyberattacken: die menschliche Firewall.

TrustMetric: Cybermaturität messen und verbessern

In unserer digital vernetzten Welt ist das Vertrauen in die Integrität und Sicherheit unserer Systeme entscheidend. TrustMetric ist ein innovativer Risikobewertungsdienst, der einen genauen Einblick in das komplexe Ökosystem von Vertrauen und Sicherheit in der Cybersphäre bietet. Unser Service ermöglicht es, die Cyberreife zu messen und kontinuierlich zu verbessern. Zudem identifiziert TrustMetric potenzielle Schwachstellen und gibt gezielte Empfehlungen, um diese zu beheben. Mit TrustMetric erkennen Sie proaktiv Schwachstellen und priorisieren Sicherheitsmassnahmen. Ausserdem vergleichen Sie den Cyberreifegrad Ihres Unternehmens automatisch mit Branchenstandards. Unser Dienst TrustMetric bietet:

- **Präzise Einblicke:** Navigieren Sie durch die verschlungenen Netze der digitalen Welt mit klaren, präzisen Einblicken, die die Nuancen von Vertrauen und Sicherheit in Ihrer Cyberumgebung aufzeigen.
- **Dynamische Bewertung der Cyberreife:** Zusätzlich zu statischen Bewertungen erleichtert TrustMetric die fortlaufende Messung und Verfeinerung der Cyberreife Ihrer Organisation. TrustMetric passt sich dabei an die sich entwickelnde digitale Landschaft an.
- **Priorisierte Aktionspläne:** Im weiten Feld der Cybersicherheit können nicht alle potenziellen Bedrohungen gleichzeitig angegangen werden. TrustMetric hilft Ihnen, Prioritäten zu setzen, damit Sie Ihre Ressourcen dort einsetzen können, wo sie die grösste Wirkung entfalten.
- **Benchmarking mit den Besten:** Stellen Sie Ihren Cyberreifegrad automatisch den Branchen-Benchmarks gegenüber und erhalten Sie eine klare Perspektive, wo Sie in der Branche stehen.

Mit TrustMetric an Ihrer Seite reagieren Sie zum einen auf die Herausforderungen der digitalen Welt und verstärken zum anderen proaktiv Ihre Cyberverteidigung. Erleben Sie die nächste Stufe der Cybersicherheitsreife mit TrustMetric von SPIE.

CISOaaS: Aufbau Ihrer Sicherheitsstrategie

Der Service CISOaaS bietet eine dynamische Lösung für Unternehmen, die eine erstklassige Führungskraft für Cybersicherheit suchen. Er überbrückt die Lücke, indem er Unternehmen bei Bedarf Zugang zu erstklassiger CISO-Expertise bietet: ohne die langfristige Verpflichtung oder den Aufwand einer Vollzeit-Führungsposition.

Hauptmerkmale von CISOaaS von SPIE

- **Fachwissen in Ihrer Hand:** Nutzen Sie das Wissen und die Erfahrung erfahrener Sicherheitsexpertinnen und Sicherheitsexperten, die an der Spitze der Cybersicherheitsstrategie und -ausführung stehen.
- **Skalierbare Lösungen:** Egal ob Ihre Organisation ein wachsendes Start-up oder ein etabliertes Unternehmen ist: Unser CISOaaS passt sich Ihren Bedürfnissen an und liefert massgeschneiderte Einblicke und Anleitungen.
- **Kosteneffizient:** Vermeiden Sie die Kosten, die mit der Einstellung einer Vollzeit-Führungskraft verbunden sind, und profitieren Sie gleichzeitig von erstklassigem Fachwissen. Dabei entscheiden Sie selbst den Grad des Engagements, der Ihrem Budget und Ihren Anforderungen entspricht.
- **Ganzheitliche Sicherheitsüberwachung:** Von Risikobewertungen und der Formulierung von Sicherheitsrichtlinien über die Planung der Reaktion auf Vorfälle bis hin zur Einhaltung gesetzlicher Vorschriften − unsere CISO-Expertinnen und -Experten geben Ihnen einen umfassenden Überblick über die Cybersicherheit in Ihrem Unternehmen.
- **Nahtlose Integration:** Unsere Expertinnen und Experten lassen sich mühelos in Ihre bestehenden Teams integrieren. Sie sorgen für einen kollaborativen Ansatz, um die Sicherheitslage Ihres Unternehmens zu verbessern.
- **Bleiben Sie auf dem Laufenden**: Mit dem CISOaaS von SPIE sind Sie der Zeit immer einen Schritt voraus. Profitieren Sie von kontinuierlichen Updates zu neu auftretenden Bedrohungen, aktuellen Best Practices und sich entwickelnden gesetzlichen Vorschriften.
- **Vertraulichkeit und Vertrauen:** Seien Sie versichert, dass bei uns Vertraulichkeit Priorität hat. Vertrauen Sie auf die tadellose Erfolgsbilanz von SPIE im Umgang mit sensiblen Informationen

CISOaaS vereint erstklassiges Fachwissen ohne Gemeinkosten. Es stellt Unternehmen aller Grössen und Branchen Führungskräfte in der Cybersicherheit zur Seite.

Schwachstellenmanagement: Berücksichtigung des Lebenszyklus von Assets

Das Schwachstellenmanagement ist ein systematischer Prozess, der in der Cybersicherheit eingesetzt wird, um Sicherheitsschwachstellen in Computersystemen und Software zu identifizieren, zu bewerten, zu priorisieren und zu entschärfen. Das Hauptziel ist es, das Risiko von Sicherheitsverletzungen zu verringern, indem bekannte Schwachstellen proaktiv behoben werden. Zu den wichtigsten Schritten des Schwachstellenmanagements gehören die Identifizierung, Bewertung, Priorisierung, Behebung, Überprüfung, Berichterstattung und kontinuierliche Überwachung. Dazu gehören auch die Patch-Verwaltung, das Sicherheitsbewusstsein und die Einhaltung von Vorschriften. So hilft das Schwachstellenmanagement Unternehmen, eine sichere IT-Umgebung aufrechtzuerhalten und die potenziellen Auswirkungen von Sicherheitsvorfällen zu minimieren.

SPIE unterstützt Sie dabei helfen, das Vorgehen des Schwachstellenmanagements für Ihr Unternehmen zu definieren und die entsprechenden Aktivitäten mit geeigneten Tools zu verfolgen.

Netzwerk-Zugangskontrolle: autorisierten Zugang sicherstellen

Da digitale Netzwerke immer komplizierter werden, ist der Schutz ihrer Grenzen sehr wichtig. Hierfür agiert die «Network Access Control» von SPIE als wachsamer Torwächter. Network Access Control (NAC) ist ein Sicherheitsansatz, der sicherstellt, dass nur autorisierte und konforme Geräte und Benutzerinnen und Benutzer auf ein Netzwerk zugreifen können. Durch die Durchsetzung von Richtlinien und Protokollen schützt NAC vor unbefugtem Zugriff, verbessert die Netzwerktransparenz und mindert Sicherheitsrisiken. Es umfasst Geräteauthentifizierung, Benutzeridentifizierung und Endpunktbewertung, um sicherzustellen, dass nur vertrauenswürdige Entitäten eine Verbindung zum Netzwerk herstellen können. Dadurch verhindert NAC, dass potenzielle Bedrohungen und Schwachstellen die Integrität und Datensicherheit des Netzwerks beeinträchtigen.

Vertrauen Sie darauf, dass SPIE die Unantastbarkeit Ihres Netzwerks aufrechterhält und Ihre Daten und Ressourcen vor unbefugten Eingriffen schützt.

Multi-Faktor-Authentifizierung: Verstärkung der Benutzerauthentifizierung

Da sich die Cyberbedrohungen stetig weiterentwickeln, ist ein einfacher Passwortschutz nicht mehr ausreichend. Als Lösung bietet SPIE die «Multi-Faktor-Authentifizierung» (MFA). Dieses Angebot ist Ihre erweiterte Verteidigungslinie. MFA erhöht nämlich die Sicherheit erheblich, indem es über das Passwort hinaus eine zusätzliche Schutzebene hinzufügt, die es unbefugten Benutzerinnen und Benutzern erschwert, Zugang zu sensiblen Informationen und Systemen zu erhalten − selbst wenn sie das Passwort

kennen. Ob Biometrie, Sicherheits-Token oder SMS-Codes − SPIE bietet eine Reihe von Authentifizierungs-Tools, die auf die individuellen Bedürfnisse jedes Unternehmens zugeschnitten sind. Diese Tools lassen sich in drei Kategorien einteilen: etwas, das Sie wissen (wie ein Passwort oder eine PIN), etwas, das Sie haben (wie ein Smartphone oder eine Smartcard), und etwas, das Sie sind (biometrische Daten wie Fingerabdrücke oder Gesichtserkennung).

Ein nahtloses Benutzererlebnis steht immer im Zentrum: Die Sicherheit wird erhöht, während der Authentifizierungsprozess benutzerfreundlich bleibt und einen schnellen Zugriff auf das jeweilige Programm erlaubt. Vertrauen Sie SPIE die Verbesserung der Zugangssicherheit in Ihrem Unternehmen an: Wir verbinden einen robusten Schutz mit Benutzerfreundlichkeit.

DNS-Sicherheit: Schutz der Domain-Integrität

Das Domain Name System (DNS) ist in der digitalen Welt ein entscheidender Wegweiser, der den Datenverkehr leitet und eine nahtlose Konnektivität gewährleistet. Das DNS muss gesichert werden, da es von Angreifern ausgenutzt werden kann, um Dienste zu stören, Benutzerinnen und Benutzer auf bösartige Websites umzuleiten oder die Datenintegrität zu gefährden. Das Angebot «DNS Security» von SPIE schützt Ihre Domain:

- **DNS-Filterung und Inhaltskontrolle:** Dadurch filtern wir bösartige oder unerwünschte Inhalte heraus, z. B. Malware, Phishing-Websites und Botnet Command-and-Control-Server. Die DNS-Filterung und Inhaltskontrolle verhindern, dass Benutzerinnen und Benutzer auf schädliche Websites zugreifen, indem sie die DNS-Auflösung für bösartige Domänen blockieren.
- **DNS-Firewall:** DNS-Firewall-Lösungen untersuchen den DNS-Datenverkehr auf Anzeichen bösartiger Aktivitäten, einschliesslich verdächtiger Domänennamen und IP-Adressen. Sie können den Zugang zu bekannten bösartigen Websites blockieren und Warnmeldungen für weitere Untersuchungen generieren.
- **Integration von Bedrohungsdaten:** Unsere «DNS Security» integriert Threat-Intelligence-Feeds, um über neu auftretende Bedrohungen und bösartige Domänen auf dem Laufenden zu bleiben. Diese Feeds helfen, bösartige Websites in Echtzeit zu identifizieren und zu blockieren. Unser Partner für DNS-Sicherheit ist Cisco, der eine umfassende Umbrella-Suite anbietet.

Mit SPIE gehen Sie sicher, dass Ihre Domain ein vertrauenswürdiger und zuverlässiger Leuchtturm in der digitalen Welt bleibt, frei von Störungen und Schwachstellen.

Segmentierung und Mikrosegmentierung: Angriffsflächen einschränken

In dem komplizierten Geflecht moderner Netzwerke sind Grenzen wichtig. Die Segmentierung von Netzwerken erhöht die Sicherheit, indem sie den Netzwerkverkehr kontrolliert und isoliert, die Auswirkungen von Sicherheitsvorfällen reduziert und die

Angriffsflächen minimiert. Das SPIE-Angebot «Segmentierung und Mikrosegmentierung» verfeinert diese Grenzen auf eine nahezu perfekte Klarheit.

Zu den Techniken des Angebots gehören virtuelle LANs (VLANs), Subnetting, Firewalls, Router und Zugriffskontrolllisten (ACLs). SPIE hat sich auf die Mikrosegmentierung spezialisiert, die besonders für die Sicherung moderner, verteilter Anwendungen in Rechenzentren oder Cloud-Umgebungen von Vorteil ist, in denen die herkömmliche perimeterbasierte Sicherheit weniger effektiv ist. Bei der Mikrosegmentierung werden häufig Software-Defined-Networking-Lösungen (SDN) oder Netzwerksicherheits-Appliances eingesetzt.

Statten Sie Ihr Unternehmen mit dem Fachwissen von SPIE aus. So verwandeln Sie Ihr weitläufiges Netzwerk in ein Labyrinth, in dem ein unbefugter Zugriff nicht nur schwierig, sondern nahezu unmöglich ist.

Identitätsüberwachung: Kontrolle der Benutzeridentifikation

Im Zeitalter der digitalen Vernetzung ist der Schutz individueller Identitäten zentral, um die Sicherheit Ihres Unternehmens zu gewährleisten. Das Angebot «Identity Monitoring» von SPIE ist Ihr umfassender Schutzschild.

Bei der Identitätsüberwachung geht es um die aktive Verfolgung und Verwaltung von Benutzeridentitäten und den damit verbundenen Zugriffsrechten innerhalb der Computerumgebung eines Unternehmens. Die kontinuierliche Überwachung und Analyse von Benutzeraktivitäten, Berechtigungen und Authentifizierungsmechanismen ist für die Sicherheit und Einhaltung von Vorschriften unerlässlich. Zu den wichtigsten Funktionen gehören die Verwaltung von Benutzerkonten, die Zugriffskontrolle, die Authentifizierung, die Prüfung und Protokollierung, die Erkennung von Anomalien, die Erstellung von Berichten über die Einhaltung von Vorschriften, die Verwaltung von Passwörtern sowie Single Sign-On (SSO) und Identitätszusammenschlüsse.

Mit SPIE am Ruder führen Sie eine Sicherheitskultur ein, in welcher die Benutzerinnen und Benutzer im Mittelpunkt stehen. Diese Sicherheitskultur sorgt dafür, dass die digitale Identität jeder einzelnen Person unangetastet und vertrauenswürdig bleibt. SPIE konzentriert sich dabei auf Privileged Access Management in Zusammenarbeit mit den Partnern Wallix und Fortinet.

Endpunkterkennung und -reaktion: Endpunktsicherheit gewährleistet

In einer Welt ausufernder digitaler Netzwerke gehören Endpunkte − von Laptops bis zu mobilen Geräten − zu den schwächsten Gliedern. Das Angebot «Endpoint Detection and Response» (EDR/XDR) von SPIE stärkt diese kritischen Knotenpunkte:

- **Proaktive Bedrohungsjagd**
- **Analyse in Echtzeit**
- **Automatisierte Reaktion & ganzheitliche Einsicht**

EDR/XDR von SPIE scannt kontinuierlich und in Echtzeit Anzeichen einer Gefährdung. Es erkennt, untersucht und reagiert auf fortschrittliche Bedrohungen und Sicherheitsvorfälle auf der Endpunktebene. Zudem überwacht es kontinuierlich Aktivitäten, sammelt und analysiert Daten von Endpunkten, liefert Details zur Untersuchung von Vorfällen, unterstützt Reaktionsmassnahmen, bietet Endpunkttransparenz, ermöglicht die Suche nach Bedrohungen, erleichtert forensische Analysen und lässt sich in andere Sicherheitslösungen integrieren.

SPIE arbeitet für sein EDR/XDR-Angebot mit Cynet, Fortinet und anderen Unternehmen zusammen. Gehen Sie eine Partnerschaft mit SPIE ein, um sicherzustellen, dass jedes Gerät in Ihrem Netzwerk zu einer uneinnehmbaren Festung wird.

Netzwerkerkennung und -reaktion (NDR): Analyse des Netzwerkverkehrs

Es ist wichtig, dass jedes Byte an Daten, das durch ein Netzwerk fliesst, sicher und unversehrt bleibt. Mit dem Angebot «Network Detection and Response» (NDR) von SPIE erhalten Sie einen wachsamen Aufseher über Ihre Datenströme.

NDR von SPIE überwacht den Netzwerkverkehr auf bösartige Aktivitäten, Anomalien und potenzielle Bedrohungen. Es bietet Einblick in den Netzwerkverkehr, ermöglicht die Suche nach Bedrohungen, unterstützt die Untersuchung von Vorfällen, ermöglicht Reaktionsmassnahmen und gewährleistet einen umfassenden Überblick über das gesamte Unternehmensnetzwerk.

Mit diesem Angebot von SPIE versetzen Sie Ihre Organisation in die Lage, die digitale Welt mit Zuversicht zu durchqueren. Sie haben dabei die Gewissheit, dass jede Welle von Daten überwacht, analysiert und geschützt wird. Die bevorzugten NDR-Partner von SPIE sind Cisco mit Stealthwatch und Fortinet.

AD-Wiederherstellung: Wiederherstellung der Integrität von Active Directory

Die Wiederherstellung von Active Directory (AD) ist für Entscheidungsträger in Unternehmen sehr wichtig, da dies die Verfügbarkeit und Integrität wichtiger Identitäts- und Zugangsverwaltungsdienste sicherstellt. Nach einem Sicherheitsvorfall ermöglicht AD Directory die Schadensbegrenzung und die Erhaltung der Integrität der AD-Objekte. Dies beinhaltet die Wiederherstellung von Benutzerkonten, Gruppenrichtlinien, Sicherheitseinstellungen und anderen netzwerkbezogenen Informationen. Die AD-Wiederherstellungsdienste und -lösungen von SPIE umfassen:

- **Schnelle Wiederherstellung:** Sollte Ihr Active Directory beschädigt oder böswillig verändert werden, gewährleistet SPIE die schnelle Wiederherstellung eines bekannten, sicheren Zustands und minimiert Ausfallzeiten und Betriebsunterbrechungen.

- **Snapshot-Funktionen:** In regelmässigen Abständen werden Snapshots der AD-Umgebung erstellt, die ein flexibles Rollback auf einen bevorzugten Zustand ermöglichen. Zudem stellen sie die Datengenauigkeit und Betriebskonsistenz sicher.
- **Prüfprotokolle:** Durch die umfassende Protokollierung aller AD-Änderungen vergewissern wir uns, dass Sie einen klaren Überblick darüber haben, was wann und von wem geändert wurde. Das erleichtert es, zu ermitteln und Verantwortlichkeiten zuzuteilen.
- **Proaktive Überwachung**: Über die Wiederherstellung hinaus überwacht unser Angebot Ihr Active Directory kontinuierlich auf Anzeichen von AD-Manipulationen oder auf potenzielle Schwachstellen. Das erlaubt vorbeugende Massnahmen, bevor eine Krise entsteht.

Wählen Sie SPIE als Ihren Partner für die AD-Wiederherstellung. Kontaktieren Sie unser Expertenteam über info.ch@spie.com

Sichern und Wiederherstellen: Schutz der Verfügbarkeit und Integrität von Daten

In der digitalen Welt sind Daten ein Vermögenswert und das Lebenselixier Ihres Unternehmens. Der Schutz dieser Daten und ihre schnelle Wiederherstellung im Falle eines Unglücks sind für die Geschäftskontinuität, die Einhaltung von Vorschriften und den Schutz vor verschiedenen Bedrohungen essenziell. Darüber hinaus minimiert eine Sicherungssoftware im Falle eines Datenverlusts oder Systemausfalls die Ausfallzeiten (Wang & Li, 2017). Zudem gewährleistet eine solche Software die Vertraulichkeit, Integrität und Verfügbarkeit von Daten während der Sicherung und Speicherung.

SPIE bietet verschlüsselte, redundante Back-ups Ihrer wichtigen Daten. Durch dieses Angebot werden die Daten einerseits sicher gespeichert, andererseits vor Beschädigung und externen Bedrohungen geschützt. Im Falle einer Sicherheitsverletzung sorgt SPIE für eine rasche Wiederherstellung Ihres Betriebs. Abgestimmt auf Ihre Bedürfnisse bietet SPIE sowohl lokale als auch Cloud-basierte Speicherlösungen an, die sicherstellen, dass Ihre sicher und zugänglich und mit den Richtlinien Ihres Unternehmens vereinbar sind.

Unser bevorzugter Partner für sichere Back-ups ist Rubrik. Kontaktieren Sie uns: Wir sind gerne ihr digitaler Wächter.

Websicherheit: Schutz von Webressourcen

In einer Zeit, in der Unternehmen online agieren und florieren, sind die Integrität und Sicherheit ihrer Webressourcen nicht verhandelbar. Als Entscheidungsträger sollten Sie die Websicherheit zu einer Ihrer Prioritäten machen, denn sie spielt eine entscheidende Rolle beim Schutz sensibler Daten, bei der Aufrechterhaltung des Kundenvertrauens und bei der Absicherung gegen Cyberbedrohungen.

Die «Web Security» von SPIE schützt Ihre digitale Präsenz:

- **Erkennung von Bedrohungen in Echtzeit:** SPIE nutzt fortschrittliche Algorithmen und Bedrohungsdaten, um kontinuierlich nach Bedrohungen für Ihre Webressourcen zu suchen und diese zu neutralisieren. So wird ein unterbrechungsfreier Onlinebetrieb gewährleistet.
- **Inhaltsfilterung:** Halten Sie böswillige oder unangemessene Inhalte in Schach. SPIE unterstützt Sie bei der Durchsetzung von Unternehmensrichtlinien und Compliance-Anforderungen und sorgt für eine sichere und professionelle Webumgebung.
- **Sichere Web-Gateways:** Dank SPIE wird jede Datentransaktion zwischen Ihrer Website und deren Besucherinnen und Besuchern verschlüsselt und abgeschirmt. Das verhindert Datenmissbrauch und Man-in-the-Middle-Angriffe.
- **Dedizierter DDoS-Schutz:** Da DDoS-Angriffe immer häufiger und raffinierter werden, bietet das Angebot «Web Security» spezielle Schutzmassnahmen, die sicherstellen, dass Ihre Onlineplattformen auch bei koordinierten Angriffen erreichbar bleiben.

Entscheiden Sie sich für «Web Security», um sicher durch die digitale Welt zu navigieren und zu wissen, dass jede Facette Ihrer Onlinepräsenz gestärkt, geschützt und kontinuierlich überwacht wird.

E-Mail-Sicherheit: Verteidigung gegen E-Mail-Bedrohungen

E-Mails sind nach wie vor das wichtigste Mittel, um in Unternehmen zusammenzuarbeiten und zu kommunizieren. Deshalb sind E-Mails ein beliebtes Einfallstor für Cyberbedrohungen. Das Angebot «E-Mail-Sicherheit» bezieht sich auf eine Reihe von Massnahmen und Protokollen zum Schutz der E-Mail-Kommunikation vor unbefugtem Zugriff, Datenschutzverletzungen, Phishing-Angriffen, Malware-Verbreitung und anderen Cyberbedrohungen. Das Angebot umfasst verschiedene Technologien, Richtlinien und Praktiken, die darauf abzielen, sowohl den Inhalt als auch die Übertragung von E-Mails zu schützen.

Das Angebot ist darauf zugeschnitten, den kritischen Kommunikationskanal zuverlässig zu schützen und bietet Folgendes:

- **fortschrittlichen Schutz vor Bedrohungen**
- **Anti-Spam-Filter**
- **Verhinderung von Datenlecks**
- **E-Mail-Verschlüsselung**

Die Implementierung von robusten E-Mail-Sicherheitsmassnahmen reduziert das Risiko von Sicherheitsvorfällen in Ihrem Unternehmen. Zudem bieten diese Massnahmen greifbare Vorteile, einschliesslich Kosteneinsparungen und verbesserte Produktivität, ob vor Ort oder in der Cloud. SPIE ICS arbeitet mit Cisco, Fortinet und Checkpoint zusammen, um einen fortschrittlichen Schutz vor E-Mail-Bedrohungen zu bieten.

Verwaltung von Sicherheitsrichtlinien: Sicherstellung der Konsistenz und Einhaltung von Richtlinien

Die Aufrechterhaltung konsistenter und konformer Sicherheitsrichtlinien ist für den Schutz der Vermögenswerte und des Rufs Ihres Unternehmens bedeutsam.

Die Verwaltung von Sicherheitsrichtlinien bezieht sich auf die systematische Planung, Implementierung, Überwachung und Durchsetzung von Sicherheitsrichtlinien innerhalb des Informationssicherheitsrahmens eines Unternehmens. Diese Richtlinien definieren die Regeln, Richtlinien und Best Practices, die festlegen, wie ein Unternehmen seine digitalen Ressourcen schützt, den Zugriff verwaltet und Sicherheitsrisiken mindert. Das Angebot von SPIE für das Management von Sicherheitsrichtlinien ist darauf ausgelegt, die Sicherheitsprotokolle im gesamten Unternehmen zu rationalisieren, zu standardisieren und ihre Einhaltung zu gewährleisten. SPIE bietet Ihrem Unternehmen folgende Vorteile:

- **Verbesserte Sicherheitslage:** Durch einheitliche und konforme Sicherheitsrichtlinien stärken Sie die Abwehrkräfte Ihres Unternehmens gegen potenzielle Bedrohungen.
- **Effizienz und Kosteneinsparungen:** Reduzieren Sie den Zeit- und Ressourcenaufwand für manuelle Richtlinienprüfungen und Audits. Das führt zu erheblichen Kosteneinsparungen.
- **Einhaltung gesetzlicher Vorschriften:** Bleiben Sie den sich entwickelnden gesetzlichen Anforderungen voraus und halten Sie sie ein, um potenzielle rechtliche und finanzielle Konsequenzen zu minimieren.
- **Informierte Entscheidungsfindung:** Mit einem klaren Verständnis Ihrer Sicherheitsrichtlinien fällen Sie strategische Entscheidungen, die mit den Unternehmenszielen und der Risikotoleranz übereinstimmen.
- **Vertrauen der Stakeholder:** Setzen Sie sich proaktiv für die Cybersicherheit ein und gewinnen Sie dadurch das Vertrauen von Interessengruppen, Partnern sowie Kundinnen und Kunden.

Das Angebot von SPIE für die Verwaltung von Sicherheitsrichtlinien gewährleistet zum einen eine konsistente Umsetzung der Richtlinien. Zum anderen gibt es Ihnen ein dynamisches Tool an die Hand, dass sich gleichzeitig mit der sich verändernden Cybersicherheit weiterentwickelt.

Firewall der nächsten Generation (NGFW): Durchsetzung der globalen Sicherheit

Da Cyberbedrohungen immer komplexer und umfangreicher werden, reichen herkömmliche Firewalls nicht mehr aus. Wir stellen Ihnen die Next Generation Firewall (NGFW) vor − eine fortschrittliche Lösung, die für die aktuellen Sicherheitsherausforderungen entwickelt wurde und gleichzeitig globalen Schutz für Ihr Unternehmen bietet.

Die Next Generation Firewall (NGFW) von SPIE ist ein hochentwickeltes Netzwerksicherheitsgerät, das herkömmliche Firewall-Funktionen mit fortschrittlichen Sicherheitsfunktionen wie Intrusion Prevention, Application Awareness und Deep Packet Inspection kombiniert. NGFWs sind so konzipiert, dass sie umfassenden Schutz vor einer Vielzahl von Cyberbedrohungen bieten, darunter Malware, Phishing und Advanced Persistent Threats (APTs).

Angesichts der sich ständig weiterentwickelnden Cyberbedrohungen ist die Next Generation Firewall von SPIE ein Leuchtturm des modernen Schutzes, der auf Unternehmen zugeschnitten ist, die globale Sicherheit ungehindert durchsetzen wollen. Mit der NGFW von SPIE navigieren Sie sicher durch die digitale Welt, denn Sie wissen, dass jedes Datenpaket, jede Anwendung und jede Benutzeraktivität genauestens überwacht wird.

SPIE ICS bietet NGFW-Lösungen für alle Anwendungsfälle in Zusammenarbeit mit den Partnern Fortinet und Checkpoint.

Fernzugriff (VPN): Sicherer Zugriff von jedem Ort aus

Da heutzutage viele Unternehmen nicht mehr nur an einen Ort gebunden sind und die Belegschaft immer mobiler wird, muss der Fernzugriff auf das Unternehmensnetzwerk sicher sein. Die Remote Access (VPN) Lösung von SPIE stellt sicher, dass Ihr Team von jedem Ort der Welt aus sicher auf wichtige Geschäftsdaten zugreifen kann.

Remote Access (VPN) bezieht sich auf die Technologie und Praktiken, die es Benutzerinnen und Benutzern ermöglichen, sich von einem entfernten Standort aus sicher mit einem privaten Netzwerk oder dem Internet zu verbinden. VPNs schaffen einen verschlüsselten Tunnel über ein ungesichertes Netzwerk, z. B. das Internet, so dass Remote-Benutzerinnen und -Benutzer auf Ressourcen, Daten und Dienste im Unternehmensnetzwerk zugreifen können, als wären sie physisch im Büro anwesend.

VPNs bieten einen sicheren Tunnel für die Datenübertragung, der sensible Informationen schützt und Unternehmen bei der Einhaltung des Datenschutzes unterstützt.

Ihre Vorteile auf einen Blick:

- **Geschützte Datenübertragungen:** Stellen Sie sicher, dass vertrauliche Informationen beim Fernzugriff vertraulich und sicher bleiben.
- **Gesteigerte Produktivität:** Mitarbeitende können von überall und jederzeit sicher auf benötigte Ressourcen zugreifen, was die Kontinuität des Betriebs fördert.
- **Einhaltung von Vorschriften:** Erfüllen Sie die gesetzlichen Anforderungen an den Datenschutz, insbesondere beim Umgang mit sensiblen oder persönlichen Informationen.
- **Reduzierte Cybersicherheitsrisiken: Mit** fortschrittlicher Verschlüsselung und Multi-Faktor-Authentifizierung werden die mit Fernzugriffspunkten verbundenen Risiken gemindert.

- **Kostengünstig:** Reduzieren Sie den mit der physischen Infrastruktur verbundenen Aufwand und nutzen Sie gleichzeitig die Vorteile, die sich durch eine mobile Belegschaft bieten.

Das Angebot «Remote Access» (VPN) von SPIE erfüllt die modernen Anforderungen von Unternehmen, die Flexibilität ohne Kompromisse bei der Sicherheit benötigen. Ermöglichen Sie es Ihrem Team, über die Grenzen des Büros hinaus zu arbeiten, in der Gewissheit, dass die hochmoderne VPN-Technologie von SPIE jede digitale Interaktion schützt.

SPIE ICS gewährleistet einen sicheren Fernzugriff in Zusammenarbeit mit den Partnern Cisco, Fortinet und Ivanti.

Intrusion Detection und Prevention (IDS/IPS): Erkennen und Blockieren von Bedrohungen

Die blosse Identifizierung potenzieller Schwachstellen reicht nicht aus. Unternehmen müssen alle nicht autorisierten Aktivitäten innerhalb ihrer digitalen Umgebungen aktiv überwachen und umgehend darauf reagieren. Dazu ist ein robustes Intrusion Detection and Prevention System erforderlich.

Intrusion Detection and Prevention Systems (IDS/IPS) beziehen sich auf Technologien und Praktiken der Cybersicherheit, die den Netzwerkverkehr und die Systeme auf Anzeichen von unbefugten oder bösartigen Aktivitäten überwachen. Das IDS identifiziert verdächtige Muster oder Verhaltensweisen, während das IPS-Massnahmen ergreift, um potenzielle Bedrohungen in Echtzeit zu verhindern oder zu entschärfen. Die beiden Systeme spielen eine entscheidende Rolle bei der Verbesserung der Sicherheitslage eines Unternehmens. IDS/IPS-Funktionen sind in NGFWs integriert oder werden als eigenständige Appliances eingesetzt, um Bedrohungen zu erkennen und zu blockieren. Das IDS/IPS-Angebot von SPIE zeichnet sich durch seine Fähigkeit aus, potenzielle Cyberbedrohungen in Echtzeit zu erkennen und zu bekämpfen. Darüber hinaus ist unser Angebot so konzipiert, dass es sich mühelos in Ihre bestehende Infrastruktur integrieren lässt. Damit gewährleisten wir eine reibungslose und unterbrechungsfreie Implementierung.

SPIE steht Ihnen bei jedem Schritt zur Seite: Von der Ersteinrichtung bis zu kontinuierlichen Upgrades und fachkundigen Beratungen sorgt unser Team dafür, dass Ihre Abwehrmassnahmen stets auf dem neuesten Stand sind.

Referenzen

Spitalzentrum Biel

- 2 Backbones
- 3 Standorte
- ~2000 Benutzerinnen und Benutzer
- >1700 Ports
- 330 WLAN-APs

Unsere Dienstleistungen:

- Cisco-Netzwerkinfrastruktur mit LAN und WLAN-Komponenten und -Dienstleistungen
- WAN zwischen dem Standort Vogelsang und der ARB AG sowie Localmed
- SM: Service-Portal, Service-Dashboard
- Managed Security Services: Internetzugang, Websicherheit, E-Mail-Sicherheit, Netzwerkzonen (Firewall), Übergang zu Partnernetzwerken, Netzwerkzugangskontrolle
- Gemanagte UC-Infrastruktur

Kanton Bern

- ~700 Standorte
- >20’000 Ports

Unsere Dienstleistungen:

- Managed LAN-Dienste (Benutzerports, Serverports)MPLS-WAN-Dienst für 700 Standorte mit teilweisem Zugang über das Mobilfunknetz und standortübergreifende IPSec-VPN
- Verwaltetes WLAN an Standorten mit Mehrfachzugang (SSIDs)
- Fernzugangsdienst mit starker Authentifizierung
- Service-Management (Service-Portal, Service-Dashboard)
- Netzwerkdienste (DNS, DHCP, IPAM, NTP)
- Verwaltete Sicherheitsdienste: Internetzugang, Web-Sicherheit (Proxy), E-Mail-Sicherheit, Netzwerkzonen (Firewall), Übergang zu Partner-Netzwerken, Netzwerkzugangskontrolle (Einführungsprojekt).
- 24/7-Servicecenter

Cybersicherheitspartner

Schlussfolgerung

Zusammenfassend lässt sich sagen, dass eine umfassende Lösung unerlässlich ist, um die verschiedenen Cyberbedrohungen, denen Unternehmen ausgesetzt sind, abzuschwächen. Es geht dabei um Technologie, um Menschen und um Prozesse, um eine robuste Verteidigung gegen die sich ständig verändernden Cyberbedrohungen zu schaffen.

In diesem globalen Überblick hat SPIE ICS sein umfangreiches Cybersicherheitsangebot vorgestellt, das eine breite Palette von Dienstleistungen und Partnerschaften umfasst. Unser Engagement für Sicherheitsprinzipien stellt sicher, dass Ihre Organisation gegenüber neuen Bedrohungen widerstandsfähig bleibt.

Cybersicherheit ist keine Einheitslösung für alle. Deshalb hat sich SPIE ICS in der Schweiz darauf spezialisiert, Lösungen auf Ihre individuellen Bedürfnisse zuzuschneiden und Ihnen die Gewissheit zu geben, dass Ihr Unternehmen geschützt ist. Wir laden Sie ein, unser Angebot näher kennenzulernen und mit uns zusammenzuarbeiten, um die digitale Zukunft Ihres Unternehmens zu sichern.

Für weitere Informationen und Anfragen kontaktieren Sie bitte info.ch@spie.com

Literaturverzeichnis

Cyllective. (2022). Penetration Testing Services. Retrieved from https://cyllective.com/penetration-testing

Johnson, K., & Lee, S. (2018). Ensuring Data Security and Compliance Through Remote Access. Journal of Information Security Management, 33(2), 164−178.

Wang, Q., et al. (2017). Minimizing Downtime with Security Backup Software. International Journal of Cybersecurity Resilience, 45(2), 153−167.